Wi-Fi Security Attacks Auditor for Wi-Fi Protected Access and Wi-Fi Protected Access-2 Protocol

Anagha M. Pilankar
M.Tech (Electronics and telecommunication)
Veermata Jijabai Technological Institute,Matunga
Mumbai, Maharashtra, India

Pankaj B. Ghate
M.Tech (Electronics and telecommunication)
Veermata Jijabai Technological Institute, Matunga
Mumbai, Maharashtra, India

***Abstract*— Wi-Fi (Wireless-Fidelity) is one of the popular wireless technology in which radio waves are used to transmit data. Wi-Fi is used extensively today and can be find every places like restaurants, railway stations, airports etc. Here data is transfer wirelessly hence more security is needed to these networks. There are mainly three security protocols are developed namely 1.Wired Equivalent Privacy 2.Wireless Protected Access 3. Wireless Protected Access-2.WEP is basic protocol and least secure among three. In this paper we will study remaining protocol in brief. But for their use, user have to write particular set of commands every time . Hence the aim of paper is to develop a software which will automate different attack. So that user can check the status of the network without doing much effort. Here we are using python language for our programming on backtrack-4 operating system. The program will first find out the encryption protocol and according to that it will perform different attack. It will generate one text file which contains key. Thus we can check the vulnerabilities of our network against different attacks and user can do modifications to enhance security.**

Keywords—WEP,WPA,WPA-2, security Attacks,python,Wi-Fi auditor,backtrack,aircrack-ng

INTRODUCTION

Wi-Fi is the Wireless Local area network (WLAN) product defined in IEEE 802.11 standard. Wi-Fi is used extensively almost in everywhere. Different devices like mobile, PDAs, laptops etc can access internet wirelessly through access points (APs).Here data is transmitted wirelessly. The attacker or unauthorized user may enter into the system and can perform some illegal activity using one's identity. Hence more security is needed to these networks. Ever since the hacking of wireless system has been on the rise different encryption system have developed for security. The three main encryption techniques are 1.WEP 2.WPA 3.WPA-2.

Among these WEP is most basic encryption and highly insecure protocol among the three.WPA is more secure than WEP while WPA2 has the highest security among three. In this paper we will study remaining two protocols and also different attacks on these protocols in detail. There are different tools available for attacking these protocols. But for its use, every time we have to go the command window and have to write particular set of commands for each of the attack. This is time consuming. So in this project we will design a software i.e. Wi-Fi auditor that will automate these attacks and will generate a report which shows status of the Wi-Fi. Thus user with no extensive background knowledge of networks can use it and can make modification to enhance security.

I. WI-FI SECURITY PROTOCOLS

A. Wired Equivalent Protocol (WEP)

WEP [6] is most basic type of encryption included in IEEE 802.11 standard in1999.This protocol is less secure [3] than others and easily breakable.

B. Wi-fi Protected Access (WPA)

This protocol is developed by Wi-Fi alliances and IEEE after WEP's vulnerabilities had been exposed and successfully attacked.

WPA [5,6] has basically two modes operation:1.WPA-PSK (Preshared Key) mode 2.WPA Enterprise mode. WPA PSK mode is similar to WEP since it requires the connecting party with a key. However this is the only similarity between this two. The PSK can be anywhere from 8 to 63 ASCII characters. It does not use master key for generating keystream , Instead of that it creates key hierarchy out of master key. This key hierarchy consists of master key and sessions keys. The master key also known as pair-wise master key (PMK) is derived from 802.1X or passphrase algorithm while session keys are derived from master key .Session keys are also known as pair-wise transient keys (PTK).This transient key is again segmented into Key Conformation Key (KCK) ,Key Encryption key (KEK) and Temporal Keys (TK).

Out of this KCK and KEK are used during the 4-way handshake and TK is used during the data session.

In PSK mode these transient keys are created dynamically when client connects to network and changed periodically. Also WPA uses Michael algorithm for data integrity replacing weak CRC32 algorithm in WEP. Michael algorithm generates message integrity check (MIC).The Access point (AP) verifies its PMK by verifying this MIC field during authentication.

In enterprise mode the PMK is created every time of user connects. This PMK is generated at the Authentication server and then transmitted down to the client. In this mode use of RADIUS server is imperative which makes the decision to accept or reject the user whereas AP completes the connection based on authentication server's decision. Once the authentication is done both client and server derive the same PMK. So overall data session consists of :

- Authentication using 802.1X or passphrase
- 4-way handshake for generating key values and exchanging keys
- Encryption is using Temporal Key integrity protocol in which RC4 is used for encryption and Michael Algorithm is used for integrity checking

Thus TKIP [2] protocol avoids attacks that can be easily done on WEP by taking following two counter majors:

- If Packet is received with incorrect ICV, an error is assumed and resulting packet is silently discarded. If ICV is correct but if MIC is incorrect then an attack is assumed and MIC failure report frames are sent to AP. If more than 2 MIC failures occur in less than 60 seconds, the communication is shut down and all keys are regenerated after 60 seconds penalty.
- After receiving each of the packets the TSC counter for that channel is updated. If packet is received out of the order the packet is discarded

But it is still breakable by chopchop, fragmentation attacksdesignations.

C. *Wi-Fi Protected Access-2*

WPA-2 [5] is the most secure encryption method of Wi-Fi network. This security standard is developed by Wi-Fi Alliance and it is implementation of IEEE 802.11i standard. This protocol uses same authentication key hierarchy and 4 way handshake like WPA. Only difference is that it uses Advanced Encryption Standard (AES) CCMP protocol for encryption instead of TKIP protocol in WPA.AES in Counter-Mode is used for encryption and AES in Cipher Block Chaining Message Authentication Code (CBC-MAC) for integrity checking. Counter Mode with CBC MAC Protocol is the most secure algorithm for Wi-Fi. CCMP uses AES block cipher algorithm which is completely different WEP and TKIP algorithms. A packet of WPA-2 consists of a packet number a header, encrypted data and MIC. There are no known realistic weakness in AES , hence previously known attacks on WEP and WPA do not work on it.

II. DIFFERENT ATTACKS ON WI-FI

A. *Deauthentication Attack*

The attack is performed by sending deauthentication packets to client .The objective for sending deauthentication packets is to get some information about network which are essential for attacking. We can get information like ESSID (Wi-Fi network name) which is broadcasted. Also to perform attack we need to capture handshakes, we can capture this handshake during re-authentication. The attack also generates ARP requests. This can be successful only if there are associated clients with given AP. For successful attack the attacker should be close to the clients. Some clients ignores these broadcasted deauthentication packets. In that case attacker needs to send directed deauthentication packets to particular client.

B. *Fake Authentication*

The fake authentication attack is performed on WEP protocol. This attack can perform open system and shared key authentication plus association with AP. This attack is useful when there are no associated MAC address available for attacking . It does not generate ARP packets. Also this attack cannot be performed on WPA/WPA2 enabled network. Some points should be considered during setting this MAC address. Mac address normally consist of six octets separated by colon e.g. 00:9B:6B:EC:EF:5B. The first half part(i.e. 00:9B:6B) is Organizationally Unique Identifier (OUI).It is given to device by manufacturer. The second half (i.e. EC:EF:5B) is extension identifier which is unique to each network card within specific OUI. Many AP ignores MAC address with invalid OUI number. Hence one must use valid OUI while performing fake authentication. The list of OUI can be found online and can be used for setting MAC address.

C. *Interactive Packet Replay Attack*

In this attack, attacker can inject (replay) a specific packet. There are two sources of packets to be injected. The first source is live flow from your wireless card and second source is from pcap file. Pcap file is captured packet file which can be reused. This file is generated after successful attack . In this attack we cannot inject any packet. Only certain packets can be accepted by access point which will generate new initialization vector. Hence we have to manipulate some packets to act a packet like natural one.

D. *ARP Request Replay Attack*

ARP stands for address resolution protocol.TCP/IP protocol is used to convert IP address into a physical address .Hence to obtain this physical address host have to broadcast ARP request onto the network. The host on the network which has address in request will give response by sending its physical address.

By using ARP request replay attack we can generate new initialization vector (IV). This attack listen for ARP packets and then retransmits this packets back to AP which will cause generation of new IV. The same ARP can be transmitted to AP over and over again. The ARP in turns generates ARP response repeatedly with new IV.

E. *Chopchop Attack*

This attack [8] is first released by KoreK. It uses the weakness in CRC32 checksum algorithm and lack of replay protection. It has ability to decrypt packet without knowing the master key. It uses Access point (AP) to decipher the Address resolution protocol (ARP).This attack is based upon the fact that one can flips a bit in the cipher text. The attack [9] chops off the packets last byte and assumes it 0.It then corrects the packets on the basis of guess of 0, re-encrypts it and sends back it to AP. If AP retransmits the packets because the attack is using multicast packet then attacker comes to know that guess was correct. If AP drops the

packets, the attacker guesses 1 and restarts the process. Hence attacker now knows the last byte of plaintext and can continue with second last byte. At the most 256 or in average 128 guesses, attacker can find out the value of last byte. For small ARP packets this attack will take 10 to 20 seconds. But for large packets its practical use is limited due to lack of speed.

F. Fragmentation Attack

The attack is first released by Andrea Bittau [1] in 2005.WEP protocol allows to send a single packet in upto 16 fragments. Due to these we can use small size keystream for ciphering. All packets in 802.11 network has similar headers hence by eavesdropping the packet the attacker can guess first 8 bytes of clear text. As both the clear text and cipher text is known to attacker, attacker can perform XOR operation and find out 8 byte of keystream for specific IV. Consider packet of size 64 bytes, this packet can be fragmented in 16 fragments. Thus each fragment is having size of 8-byte consisting of 4 bytes of clear text and 4-byte CRC32 checksum. When these 16 fragments are received by AP, it will decipher them, combine them into single packet, encrypt it and send it back on the network. Now this packet is 68 bytes long having 64-bytes of known text and 4-bytes of ICV. Attacker now XOR this known text with cipher text to obtain 68 bytes of keystream for given IV. By repeating this process, the attacker can get up to 1500 bytes of keystream for a IV.

G. Dictionary Attack against Handshake

It exists a key-recovery attack on WPA (Pre-Shared Key version), when the key is a word from a dictionary. Attacker eavesdrops the network fist. The goal of the attacker is to get a handshake; the hash of the key swapped between the client and the AP when the client begins the connection. The attacker can wait, or launch a deauthenticate-attack against the client. When he gets the hash, he can try to and the key with a dictionary-attack, a rainbow-attack or one of the multiple attacks that exist on hashed keys in general.

III. PROGRAMING LANGUAGE AND TOOLS

We are developing this application in python language. The version used here is python 2.6.x.This language is case sensitive like c++, java etc. Source code does not declare types of variables or functions. Due to this code become short and flexible .Completion of source become fast as there no compile time type checking. The application will run on linux based Backtrack 4 operating system.

The most important program used here is aircrack-ng [7].This tool is used for performing different attack on WEP and WPA encrypted network. By using this we can crack key for WEP and WPA-PSK after capturing enough packets. Aircrack-ng is set of different tools. Some of the important tools are given below:

aireplay : This tool is used for injecting packets.

airodump:It is used as sniffing tool to find out WEP enabled network.

aircrack:Used for collecting IVs and finding WEP key.

Firstly aireplay-ng [6] listens ARP request and then reinjects this request back into network. After that, airodump is used to capture initialization vectors. Then aircrack along with other tools is used to obtain the key.

For performing any attack user need to go to the terminal and have to write set particular set of instruction each time. This is very much time consuming. Hence we are developing software which will automate all the attacks. Following are some features of this program

- It determines which encryption technique is used on given network.
- It can deauthenticate clients which are connected to hidden networks.
- It backs up all captured WPA handshakes into current directory
- Before attacking the MAC address is changed to random MAC address and after completion of attack the MAC address gets back to its original value.
- It can stop attack, go for next attack or can move for next values.
- All Cracked key values are stored in Log.text values.

IV. RESULT

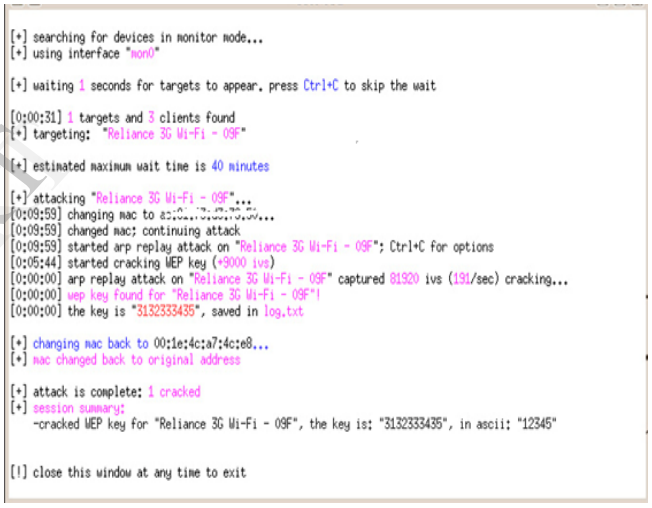

Fig.1. Successful attack on WEP in Backtrack

Fig.1.shows the successful attack on WEP protocol.In our software we have to chose the interface and attacks to be performed .We also select the type of encryption.Here it first find out access point on which this WEP protocol is running.Then attacker changes it MAC address to one of the authorised MAC address.Here Reliance 3G was attacked.Air eplay attack has been successfully performed on it..The attack took about 10-15 minutes.It gave log.text file which contains the WEP key.From this we can concluse that WEP is very much easy to attack.If air reply attack gets unsuccessful then it will go for higher attacks like chopchop and fragmentation.

Fig.2.Successful Attack on WPA in backtrack

Fig.2. shows attack on WPA network. Out of different targets obtained we have selected 5th target. After performing WPS PIN attack it has found PIN and WPA key .The attack took more than 16 hours. Hence we can conclude that WPA is more secure than WEP as it took more time for attack.

V. CONCLUSION

Thus we have studied WPA and WPA-2 protocols and attacks on those protocols briefly. We have also automated the attacks in Aircrack-ng and developed GUI in Python for Backtrack operating system. It can be seen that the WEP is easily attacked within some minutes. The WPA takes more time than WEP. It nearly takes 17 hours for cracking. The WPA-2 is the most secure protocol than others on which attacks are not performed successfully.

REFERENCES

[1] A.Bittau, M. Handley and J. Lackey. "The Final Nail in WEP's Coffin "Security and Privacy, IEEE Symposium May 2006.

[2] M. Beck, E. Tews, T. Darmstadt," Practical attacks against WEP and WPA ",2008

[3] Tsubasa TSUKAUNE, Yosuke TODO, Masakatu MORII "Proposal of a Secure WEP Operation against Existing Key Recovery Attacks and its Evaluation" Seventh Asia Joint Conference on Information Security2012

[4] E. Tews. Attacks on the wep protocol Cryptology ePrint Archive, Report 2007/471, 2007.

[5] I. P. Mavridis, A.-I. E. Androulakis, A. B. Halkias ,Ph. Mylonas"Real-life paradigms of wireless network security attacks" Panhellenic Conference on Informatics,2011

[6] S. Fahmy, A. Nasir and N. Shamsuddin "Wireless Network Attack: Raising the Awareness of Kampung WiFi Residents" Computer & Information Science (ICCIS), 2012 International Conference on (Volume:2) June 2012

[7] F. T. Sheldon , J. Mark Weber, S. Yoo, W. D. Pan "The Insecurity of Wireless Networks" Security & Privacy, IEEE (Volume:10)May 2012